Kvantu datorika

B.phys.V.Kaščejevs, 2000

Kvantu datorika pēta priekšrocības, ko dod kvantu pasaules likumu izmantošana informācijas apstrādē un pārraidē.

1. Kvantu mehānikas pamatprincipi
   - dažas atziņas no lineārās algebras
   - superpozīcija
   - mērījums

2. Kvantu sistēmas kā informācijas nesēji
   - q-bits
   - kvantu loģiskās operācijas

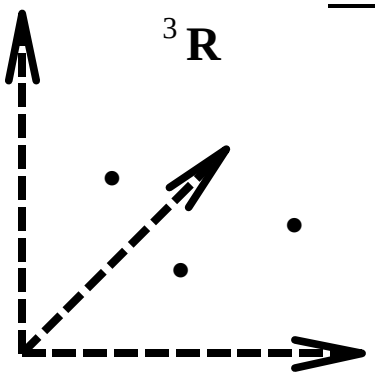
3. Pirmais pielietojums – kvantu kriptogrāfijā
   - atslēgas kvantu pārraides algoritms

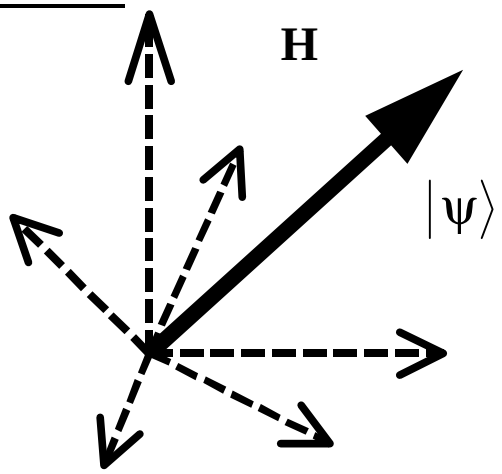
4. Vairāku q-bitu efekti
   - spītie stāvokļi *(entaglment)*
   - teleportācija
   - P.Šora faktorizācijas algoritms

5. Perspektīvas
   - kvantu datoru praktiskā reailzācija
   - ieteicamā literatūra
   - ieskaites nosacījumi

Klasiskā mehānika Kvantu mehānika

Sistēmas stāvoklis





Punktu kopa (*vairāki*)

$(\vec{r}_1, \vec{r}_2, \ldots, \vec{r}_n)$ un
$(\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n)$

reālājā 3-D
Eiklīda telpā

Stāvokļa *vektors* (*viens*)

$|\psi\rangle$

kompleksajā ∞-D
Hilberta telpā

Stāvokļa izmaiņa laikā

Punktu *pārvietošanās*

Ņūtona vienādojums

$$m_k \frac{d\vec{r}_k}{dt} = -\frac{\partial U}{\partial \vec{r}_k}$$

Stāvokļa vektora *griešanās*

Šrēdingera vienādojums

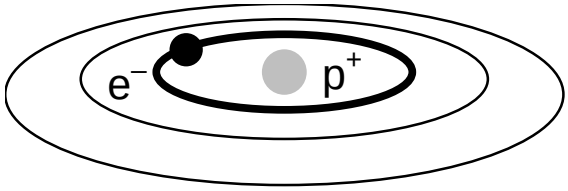
$$i\hbar \frac{\partial}{\partial t}|\psi\rangle = \hat{H}|\psi\rangle$$

Saistība strap *klasisko* un *kvantu* pasauli

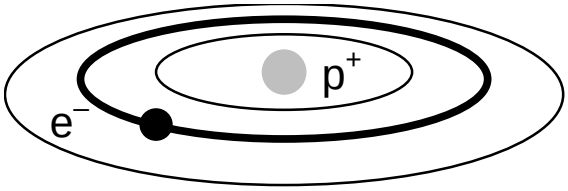
Mērījums

$$P(\vec{r}_k) = \left|\langle \vec{r}_k \,|\, \psi\rangle\right|^2$$

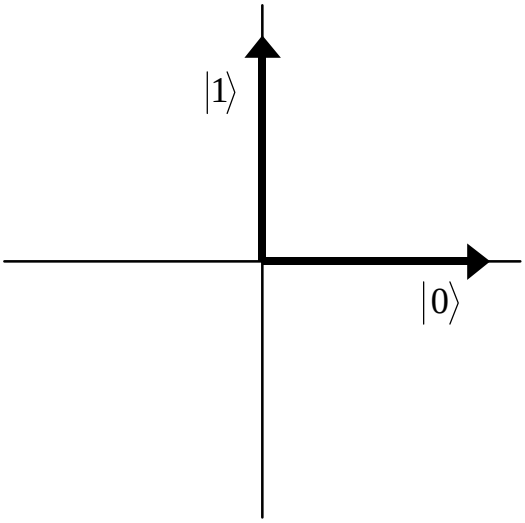
Atoma stāvokļi ar noteiktu enerģiju



Stāvoklis $|0\rangle$ ar enerģiju E_0

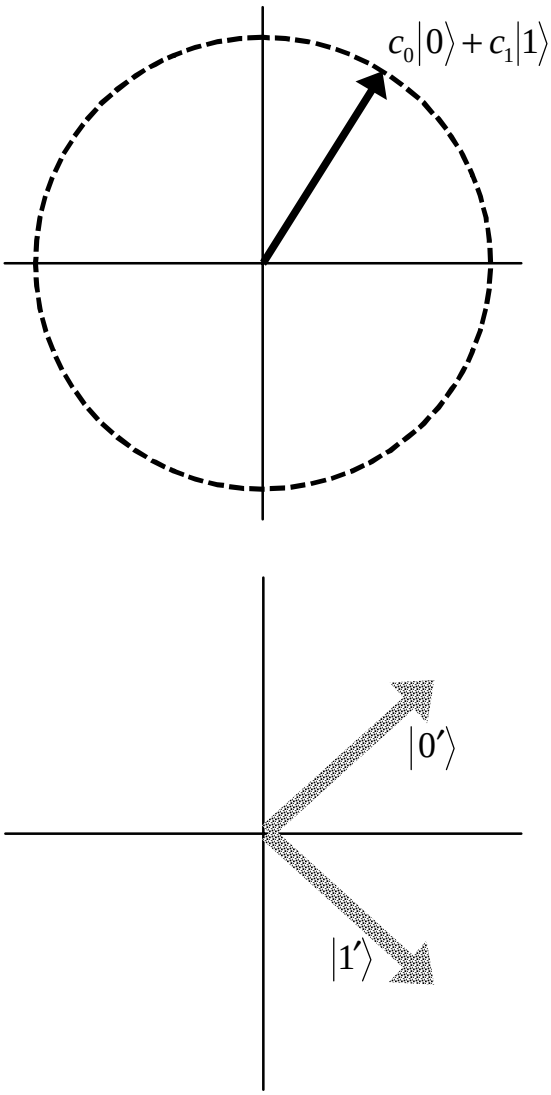


Stāvoklis $|1\rangle$ ar enerģiju E_1



Superpozīcija $|\Psi\rangle = c_0|0\rangle + c_1|1\rangle$ $\xrightarrow{\text{mērījums}}$ $\begin{cases} E_0 \text{ ar varbūtību } |c_0|^2 \\ E_1 \text{ ar varbūtību } |c_1|^2 \end{cases}$

$|c_0|^2 + |c_1|^2 = 1 \Rightarrow$ stāvokļa vektori ir normēti


$c_0|0\rangle + c_1|1\rangle$
$|0'\rangle$
$|1'\rangle$

Hilberta telpas īpašības

- Hilberta telpa:

  Lineārā kompleksā vektoru telpa $\mathcal{H}$

  $$|\alpha\rangle, |\beta\rangle, |\gamma\rangle \ldots \in \mathcal{H}\,,$$
  $$\forall\, c_1, c_2 \in \mathbb{C}:\ c_1\,|\alpha\rangle + c_2\,|\beta\rangle \in \mathcal{H}\,,$$

  ar skalāro reizinājumu

  $$(|\alpha\rangle, |\beta\rangle) \equiv \langle\alpha|\beta\rangle \in \mathbb{C}\,.$$

  Normēšana $\langle\alpha|\alpha\rangle = 1$,

  ortogonalitātē $\langle\alpha|\beta\rangle = 0$.

- Pola Diraka apzīmējumi:

  Katrs "ket"-vektors ir saistīts ar savu "bra"-vektoru.

"bra"-vektors	$\leftrightarrow$	"ket"-vektors
$\langle\alpha\|$	$\leftrightarrow$	$\|\alpha\rangle$.
$\langle\alpha\|\beta\rangle$	ir	"bra-cket"

  Saistīšana: $|\alpha\rangle^\dagger = \langle\alpha|$,

  $$(\langle\alpha|\beta\rangle)^\dagger = |\beta\rangle^\dagger \cdot \langle\alpha|^\dagger = \langle\beta|\alpha\rangle = \langle\alpha|\beta\rangle^*$$

Teorēma. Ja ir dots normēts vektors $|\psi\rangle$ ortonormētajā bāzē
$|\psi\rangle = c_1|1\rangle + c_2|2\rangle + \ldots + c_n|n\rangle$, tad
a) $\sum_{i=1}^{n} |c_i|^2 = 1$,
b) $c_i = \langle i|\psi\rangle$.

Pierādījums. a)

$$1 = \langle\psi|\psi\rangle = |\psi\rangle^\dagger |\psi\rangle = (\sum_i c_i|i\rangle)^\dagger |\psi\rangle =$$
$$\sum_i {c_i}^\dagger |i\rangle^\dagger |\psi\rangle = \sum_i {c_i}^* \langle i| \sum_j c_j|j\rangle =$$
$$\sum_{i,j} {c_i}^* c_j \langle i|j\rangle = \sum_i {c_i}^* c_i \langle i|i\rangle = \sum_i |c_i|^2.$$

b) $$\langle i|\psi\rangle = \langle i| \sum_j c_j|j\rangle = \sum_j c_j\langle i|j\rangle = c_i.$$

Līdz ar to $\langle\psi| = \sum_i |i\rangle\langle i|\psi\rangle$.

1 **q-bits** = kvantu sistēma ar diviem stacionāriem stāvokļiem

$$\boxed{|\Psi\rangle = c_0|0\rangle + c_1|1\rangle}$$

q-bits $\overset{\text{mēram}}{\longrightarrow}$ klasiskais bits (0 vai 1).

q-bita realizācijas piemērs: fotona polarizācijas stāvokļi

$$|0\rangle \equiv |\leftrightarrow\rangle,\ |1\rangle \equiv |\updownarrow\rangle$$

Superpozīciju piemēri:

$$\begin{aligned}
|\nearrow\swarrow\rangle &= \frac{1}{\sqrt{2}}\Big(|\leftrightarrow\rangle + |\updownarrow\rangle\Big)\\
|\nwarrow\searrow\rangle &= \frac{1}{\sqrt{2}}\Big(|\leftrightarrow\rangle - |\updownarrow\rangle\Big)\\
|\circlearrowleft\rangle &= \frac{1}{\sqrt{2}}\Big(|\leftrightarrow\rangle + i\,|\updownarrow\rangle\Big)\\
|\circlearrowright\rangle &= \frac{1}{\sqrt{2}}\Big(|\leftrightarrow\rangle - i\,|\updownarrow\rangle\Big)
\end{aligned}$$

Gan $\Big\{|\leftrightarrow\rangle, |\updownarrow\rangle\Big\}$, gan $\Big\{|\nearrow\swarrow\rangle, |\nwarrow\searrow\rangle\Big\}$, gan $\Big\{|\circlearrowleft\rangle, |\circlearrowright\rangle\Big\}$ ir vienlīdz derīgas ortonormētas bāzes.

Operācijas ar q-bitiem (kvantu loģiskie vārti)

Sistēmas stāvoklis mainās laikā atkarībā no ārējiem apstākļiem (laukiem).

Uz laiku pakļaujot q-bitu noteiktai iedarbībai, var mainīt tā stāvokli.

$$|\Psi(t)\rangle = c_0(t)\,|0\rangle + c_1(t)\,|1\rangle,$$
$$\text{bet } \; |c_0(t)|^2 + |c_1(t)|^2 = 1 = \text{const.}$$

Stāvokļa vektros nemaina savu garumu (normu), bet tikai pagriežas.

Pagriezieni ir ērti aprakstāmi ar **unitāro matricu** palīdzību.

Viena q-bita operācija **NOT-vārti** $\hat{U}_{NOT}$ (klasiskā noliieguma analogs):

$$\hat{U}_{NOT}|0\rangle = |1\rangle, \quad \hat{U}_{NOT}|1\rangle = |0\rangle.$$

Vektoru pieraksta bāzē $\{|0\rangle, |1\rangle\}$ kā matricu-kolonnu:

$$|0\rangle \to \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle \to \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

$$|\Psi\rangle = c_0|0\rangle + c_1|1\rangle \to$$
$$\to c_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + c_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}.$$

Operāciju pieraksta kā 2×2 matricu:

$$\hat{U}_{NOT} \to \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} = \begin{pmatrix} c_1 \\ c_0 \end{pmatrix}$$

Cita 1 q-bita operācija — **Adamāra** (*Hadamard*) **transformācija**:

$$\hat{U}_H|0\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) = |0'\rangle$$
$$\hat{U}_H|1\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big) = |1'\rangle$$

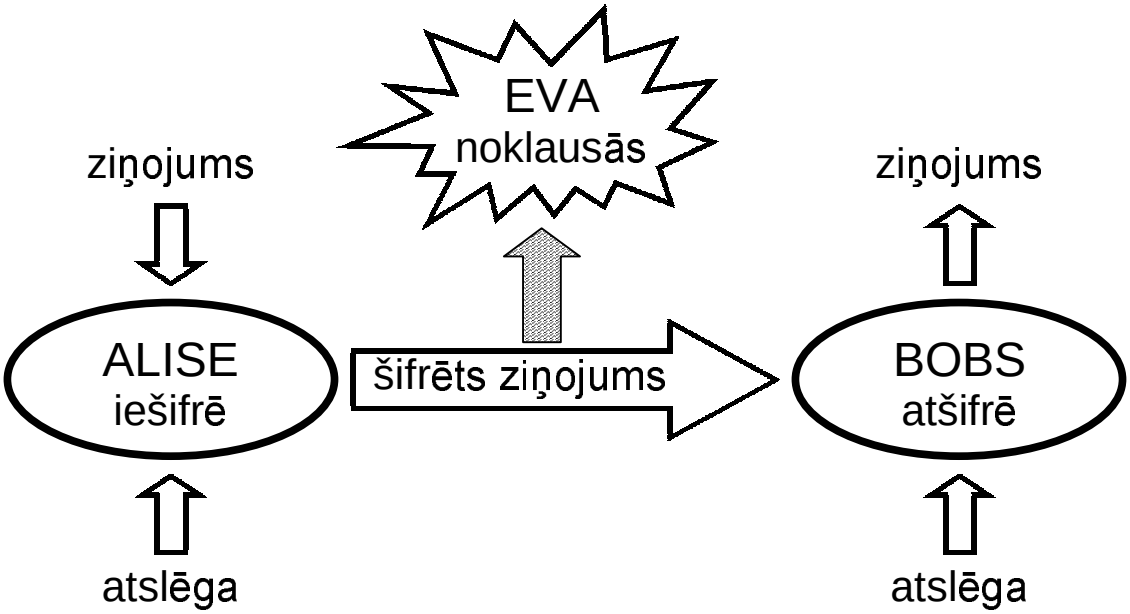
Adamāra transformāciju parasti uzlūko kā bāzes maiņu:

$$\hat{U}_H\big(c_0|0\rangle + c_1|1\rangle\big) = c_0|0'\rangle + c_1|1'\rangle$$

Matricas formā

$$\hat{U}_H \to \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Kriptogrāfijas pamatuzdevums



Kriptogrāfijas sistēmas

<u>ar slepeno atslēgu</u>
(*private key*)

- vienreizējās atslēgas algoritms (*one-time-pad*)
  Gilbert Vernam, 1935
- atslēgas kvantu pārraide (*quantum key distribution*)
  Charles Bennet,
  Gilles Brassad, 1984

<u>ar atklāto atslēgu</u>
(*public key*)

Whitefield Diffie,
Martin Hellman, 1976

- RSA kriptosistēma
  Ronald Rivest,
  Adi Shamir,
  Leonard Adleman
  1984

Vienreizējās atslēgas sistēma

Slepenā atslēga – gadījuma bitu virkne.

Iešifrēšana:

Atslēga		1	0	1	1	0	1	0	1
Ziņojums	⊕	0	1	1	0	1	0	0	1
Šifrētais ziņojums		1	1	0	1	1	1	0	0

Atšifrēšana:

Šifrētais ziņojums		1	1	0	1	1	1	0	0
Atslēga	⊕	1	0	1	1	0	1	0	1
Ziņojums		0	1	1	0	1	0	0	1

1. **ALISE un BOBs slepeni iegūst pa vienai kopijai slepenās atslēgas.**
2. **ALISE iešifrē ziņojumu, to saskaitot pēc moduļa 2 ar slepeno atslēgu.**
3. **Šifrētais ziņojums tiek pārraidīts pa atklāto kanālu BOBam.**
4. **BOBs atšifrē ziņojumu, atkārtojot ALISES veikto operāciju ar saņemto šifrēto ziņojumu.**

Vienreizējās atslēgas sistēma

\+ Vienīgā absolūtā drošā sistēma

— Slepenu atslēgu ir grūti pārraidīt

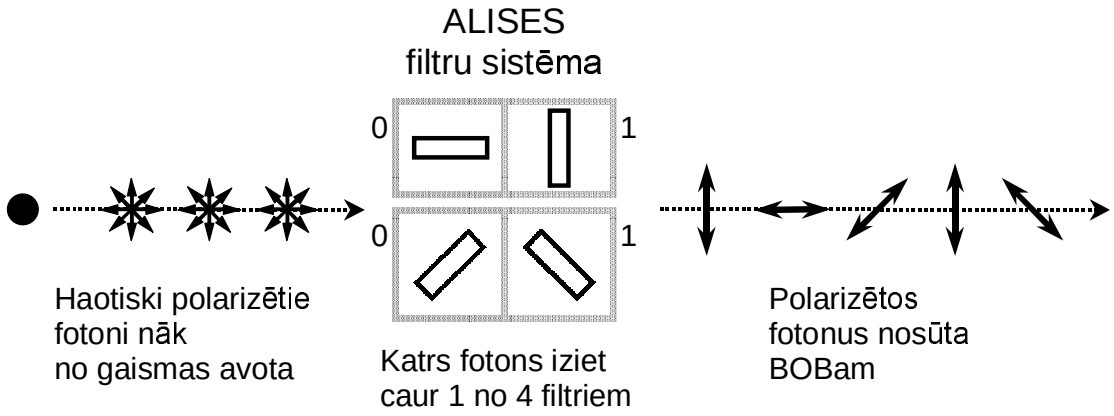
Risinājums –

Kvantu atslēgas pārraide

EVA nevarēs noklausīties nepamanīta !

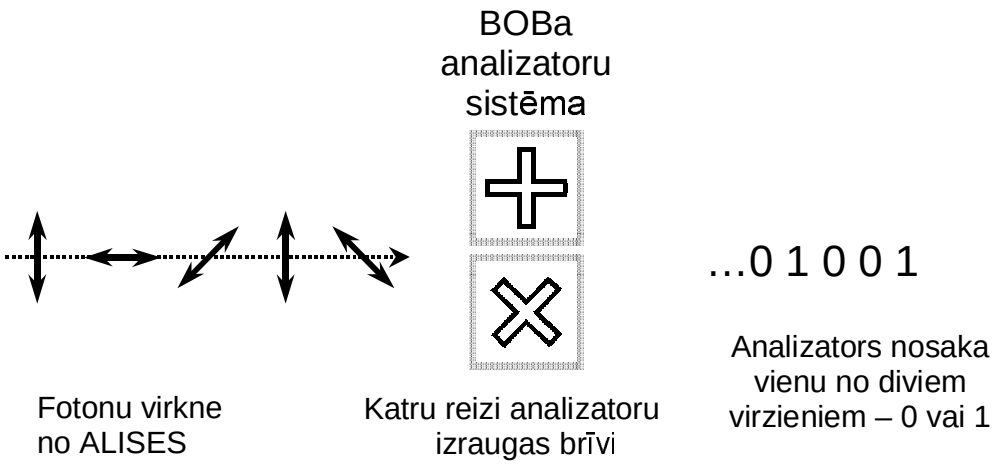
Atslēgas kvantu pārraide

(algoritms BB84)



1. ALISE nosūta BOBam virkni fotonu, katram pēc gadījuma izvēloties vienu no četriem polarizācijas virzieniem.
2. Katram fotonam ALISE pieraksta, kura no divām filtru sistēmām tika izmantota
   (vertikālā-horizontālā + vai diagonālā ×)

   …+ + × + ×



3. BOBs detektē fotonu polarizācijas virzienus, katru reizi izvēloties analizatora gadījuma analizatora tipu (+ vai ×).
4. BOBs paziņo ALISEI pa atklātu kanālu, kādus filtrus viņš ir izvēlējies (bet ne mērījumu rezultātus).
5. ALISE salīdzina informāciju no BOBa ar savu pierakstu un paziņo BOBam, kuri biti ir pārraidīti pareizi. Tie arī veido slepeno atslēgu.

ALISEs virkne	**1**	**0**	**1**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**1**	**1**	**0**
ALISEs fotoni	↕	↔	⤢	↕	⤡	⤡	⤢	↕	⤡	↔	↕	⤢	↔
BOBa filtri	+	×	+	+	×	×	+	+	×	+	×	×	+	+
BOBa mērījums	**1**	**0**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**1**	**0**	**0**
pārraidītā virkne	**1**	**–**	**–**	**1**	**0**	**0**	**–**	**1**	**0**	**0**	**–**	**1**	**–**	**0**